

明 細 書

コンテンツ配信システム

技術分野

- 5 本発明は、コンテンツを配信する技術に関し、特に、コンテンツの配信を許可する端末を判断する技術に関する。

背景技術

- 10 近年、家庭内の端末をネットワークで接続し、接続された端末間でコンテンツの共有を図る家庭内ネットワークが実現されつつある。

- 15 家庭内ネットワークの実現形態の一つとして、家庭内にルータを1台設け、そのルータ下にDVDレコーダやビデオなどの各端末と、コンテンツを蓄積するコンテンツサーバとを接続する形態が考えられる。ルータは、家庭内において唯一家庭外のネットワークに接続されており、コンテンツサーバは、ルータを介して家庭外のネットワークからコンテンツを取得し、取得したコンテンツを蓄積する。各端末は、
20 コンテンツサーバへコンテンツを要求し、コンテンツサーバは、端末からの要求に応じて、コンテンツを配信する。

- 25 しかしながら、著作権保護の観点より、コンテンツを無制限に配信することは認められない。従って、家庭内の端末のみに利用が許可されたコンテンツは、家庭外の端末に配信されないよう制限されなければならない。

そこで、特許文献1には、送信装置と受信装置とが同一のサブネットアドレスを有する場合に、認証及び鍵交換を実行してコンテンツを送受信する技術が開示されている。

- 30 上記の技術により、同一のサブネットアドレスを有する端末間でのみ、コンテンツを送受信することが可能であるが、同一のサブネットアドレスを有する端末間であっても、通信途中で第三者にコンテンツを盗まれる危険度が高い状況などでは、コンテンツの送受信を抑制したいという要望がある。

【特許文献1】特開2001-285284号公報

発明の開示

そこで、本発明は、上記の要望に鑑みなされたものであって、通信途中で第三者にコンテンツを盗まれる危険度が高い状況では、コンテンツの送受信を抑制するコンテンツ配信システムを提供することを目的とする。

5 上記目的を達成するために本発明は、本発明は、通信装置であって、前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得し、取得した前記通信距離が、所定値以下であるか否か判定し、前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行うことを特徴とする。

10 この構成によると、他の通信装置とのデータ通信における隔たりの量と、前記所定値とに応じてコンテンツを送受信したり、コンテンツの送受信を抑制したりできる。

15 ここで、前記通信装置は、前記コンテンツの送信又は受信に先立ち、前記他の通信装置とデータの通信を行い、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数を示す前記通信距離を取得するように構成してもよい。

この構成によると、他の通信装置とのデータ通信においてデータが経由した中継機器の数と、前記所定値とに応じてコンテンツを送受信したり、コンテンツの送受信を抑制したりできる。

20 ここで、前記通信装置は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数として、前記データが経由したルータの数を示す前記通信距離を取得するように構成してもよい。

25 この構成によると、他の通信装置とのデータ通信においてデータが経由した値ルータの数と、前記所定値とに応じてコンテンツを送受信したり、コンテンツの送受信を抑制したりできる。

ここで、前記通信装置は、ルータを一つ経由する毎に1ずつ値が減少する性質を有するTTL (Time To Live) を含むパケットの形式で、前記データの通信を行い、受信するパケットに含まれる前記TTLを用いて、前記データが経由したルータの数を示す前記通信距離を取得するように構成してもよい。

この構成によると、データが経由したルータの数を取得する取得方法として、IPパケットのTTLフィールドに設定されるTTLを用いることで、既存の通信プロトコルを用いて本発明を実施することができる。

5 ここで、前記通信装置は、更に、前記他の通信装置と鍵情報を共有するように構成してもよいし、また、前記通信装置は、更に、前記他の通信装置と共有した前記鍵情報を用いて、前記コンテンツの暗号化処理及び暗号化された前記コンテンツの復号処理を行い、前記他の通信装置との間で、暗号化された前記コンテンツの送信又は受信を行うように構成してもよい。

10 この構成によると、他の通信端末との間で鍵共有処理を行い、当該通信端末と他の通信端末との間で、共有した鍵情報を用いてセキュアにコンテンツを送受信することができる。

15 ここで、前記通信装置は、前記他の通信装置から、当該他の通信装置が接続されている第1のルータを一意に識別する第1識別情報を含む前記パケットを受信し、更に、当該通信装置が接続されている第2のルータを一意に識別する第2識別情報を取得し、前記第1識別情報と前記第2識別情報とが一致するか否か判断し、前記判断の結果が否定的である場合に前記コンテンツの送受信を抑制するように構成してもよい。

20 この構成によると、接続されている中継機器の識別情報を取得して判断することにより、確かに同一の中継機器に接続された通信装置間でコンテンツを送受信することができ、外部にコンテンツが流出するのを抑制することができる。

 ここで、前記通信装置が送受信する各パケットは、当該通信装置が接続されているネットワークの最大伝送量 (Maximum Transmission Unit) に等しいデータサイズであり、且つ、分割して送受信することが禁止されているように構成してもよい。

25 この構成によると、前記他の通信装置が、IPパケットの外側に新しいIPヘッダを付加して実際に指定された数のTTLと異なるTTLを設定して送信しようとする場合に、既にパケットがMTUに等しいサイズであるため、新たなIPヘッダを付加するとパケットを分割送信しなくてはならない。しかしながら、この構成により、パケットの分割送信は禁止されているため、結局不正なパケットは当該通信

装置に届かない。

ここで、前記通信装置は、前記他の通信装置から、送信時に所定TTLが設定されて送信されたパケットを受信し、受信した前記パケットからTTLを読み、読み出したTTLと前記所定TTLとの差分である前記通信距離を取得するように構成してもよい。

この構成によると、予め、他の通信装置に所定TTLを通知しておくことで、受信したパケットに含まれるTTLを読み出すことで、容易にデータが経由したルータの数を取得することができる。

ここで、前記通信装置は、前記他の通信装置から、送信時に前記所定TTLとして「1」が設定されて送信された前記パケットを受信するように構成してもよい。

この構成によると、他の通信装置から、TTLが「1」に設定されたパケットが送信されるため、当該通信装置が、パケットを受信した場合、前記パケットは、他のネットワークのルータを経由せずに他の通信装置から当該通信装置へ送信されたことが分かる。即ち、当該通信装置と前記他の通信端末とが同一のルータ下に接続されていることが分かる。

ここで、前記通信装置は、一部又は全部が暗号化されたパケットを送信又は受信し、受信したパケットを復号して各処理を行い、又は、送信されるパケットを暗号化して出力するように構成してもよい。

この構成によると、判定に用いるデータであるパケットの一部又は全部が暗号化されているため、前記データをセキュアに送受信することができる。

図面の簡単な説明

図1は、コンテンツ配信システム1の構成を示す図である。

図2は、コンテンツサーバ20の構成を機能的に示す機能ブロック図である。

図3は、端末30の構成を機能的に示す機能ブロック図である。

図4(a)は、コンテンツサーバ検索パケット301のデータ構造を示す図である。

(b)は、確認パケット302のデータ構造を示す図である。

(c)は、鍵共有要求パケット303のデータ構造を示す図である。

図5は、コンテンツ配信システム1の動作を示すフローチャートである。

図6は、コンテンツ配信システム1におけるAD判定処理の動作を示すフローチャートであり、図7に続く。

5 図7は、コンテンツ配信システム1におけるAD判定処理の動作を示すフローチャートであり、図6から続く。

図8は、コンテンツ配信システム1における鍵共有処理の動作を示すフローチャートである。

図9(a)は、コンテンツ配信システム1におけるコンテンツ送信処理の動作を示すフローチャートである。

10 (b)は、コンテンツ配信システム1におけるコンテンツ受信処理の動作を示すフローチャートである。

図10は、コンテンツ配信システム1aの構成を示す図である。

図11は、端末30bの構成を機能的に示す機能ブロック図である。

図12は、TTL検索パケット304のデータ構造を示す図である。

15 図13は、コンテンツ配信システム1aの動作を示すフローチャートである。

図14は、コンテンツ配信システム1aにおけるTTL検索処理の動作を示すフローチャートである。

図15は、コンテンツ配信システム1aにおけるAD判定処理の動作を示すフローチャートであり、図16に続く。

20 図16は、コンテンツ配信システム1aにおけるAD判定処理の動作を示すフローチャートであり、図15から続く。

図17は、コンテンツ配信システム1bの構成を示す図である。

図18は、コンテンツサーバ20bの構成を機能的に示す機能ブロック図である。

図19は、端末30cの構成を機能的に示す機能ブロック図である。

25 図20(a)は、公開鍵パケット305のデータ構造を示す図である。

(b)は、公開鍵パケット306のデータ構造を示す図である。

図21は、コンテンツ配信システム1bの全体の動作を示すフローチャートである。

図22は、コンテンツ配信システム1bにおける鍵共有処理の動作を示すフロー

チャートである。

図 2 3 は、コンテンツ配信システム 2 の構成を示す図である。

図 2 4 は、コンテンツサーバ 2 0 a の構成を機能的に示す機能ブロック図である。

図 2 5 は、グループテーブル 3 5 0 のデータ構造を示す図である。

5 図 2 6 (a) は、コンテンツ配信システム 2 の動作を示すフローチャートである。

(b) は、コンテンツ配信システム 2 におけるコンテンツ要求処理の動作を示すフローチャートである。

発明を実施するための最良の形態

10 以下、本発明の実施の形態について詳細に説明する。

＜第 1 の実施の形態＞

本発明に係る第 1 の実施の形態として、コンテンツ配信システム 1 について図面を参照して説明する。コンテンツ配信システム 1 は、コンテンツの利用が許可された範囲において、機器間でコンテンツを送受信するシステムである。以下では、
15 コンテンツの利用が許可された範囲を「AD (Authorized Domain)」と呼称する。また、以下では、特に AD として、家庭内ネットワークに接続された家庭内の機器を想定している。

＜構成＞

図 1 は、コンテンツ配信システム 1 の構成を示す図である。同図に示す様に、
20 コンテンツ配信システム 1 は、ルータ 1 0、ルータ 1 1、ルータ 1 2、コンテンツサーバ 2 0、端末 3 0、端末 4 0 及び端末 5 0 から構成される。

インターネット 6 0 に接続されたルータ 1 0 には、ルータ 1 1 及びルータ 1 2 が接続されている。ルータ 1 1 は、AD 内に存在する中継機器であり、ルータ 1 2 は AD 外に存在する中継機器である。ルータ 1 1 には、コンテンツサーバ 2 0 と端末
25 3 0 とが接続されており、ルータ 1 2 には、端末 4 0 と端末 5 0 とが接続されている。

なお、コンテンツ配信システム 1 において、AD 内の各端末は、一つのルータ下に接続されているものとする。また、コンテンツ配信システム 1 において、各機器は通信プロトコルとして I P v 4 を使用して通信を行うものとする。

1. コンテンツサーバ20の構成

コンテンツサーバ20は、他の機器からの要求を受け、前記機器がAD内の機器であるか、又は、AD外の機器であるか判断する。判断の結果、前記機器がAD内の機器である場合に、コンテンツサーバ20は、前記機器と鍵共有処理を行い、共有した鍵を用いて暗号化したコンテンツを前記機器へ送信する。

なお、以下では、AD内の機器であると判断された端末を、「グループ内端末」又は「グループメンバ」と呼称することがある。

図2は、コンテンツサーバ20の構成を機能的に示した機能ブロック図である。同図に示す様に、コンテンツサーバ20は、通信部101、暗号処理部102、機器ID管理部103、中継機器固有情報取得部104、最大伝送量探査部105、AD判定部106、確認情報生成部107、共有鍵生成部108及びコンテンツ格納部109から構成される。

コンテンツサーバ20は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ネットワーク接続ユニット、ディスプレイユニット、リモートコントローラなどから構成されるコンピュータシステムであって、ここでは、HDDレコーダを想定している。

前記RAM又は前記ハードディスクユニットにはコンピュータプログラムが記憶されており、前記マイクロプロセッサが、前記コンピュータプログラムに従い動作することにより、コンテンツサーバ20は、各種の機能を達成する。

(1) 通信部101

通信部101は、ルータ11を介してIPパケットを送受信することにより他の機器と通信を行う通信インターフェースである。

通信部101は、暗号処理部102によりIPペイロードが暗号化された送信用パケットを順次受け取り、受け取った送信用パケットをルータ11へ送出する。送信用パケットの一例は、図4(b)に示した確認パケット302である。また、通信部101は、暗号処理部102により暗号化された送信情報を受け取り、受け取った送信情報を分割して送信用パケットを生成し、生成した送信用パケットを順次ルータ11へ送出する。送信情報の具体例は、暗号化コンテンツ、コンテンツサーバ20の公開鍵等である。なお、通信部101は、送信情報を分割して送信用パケ

ットを生成する際、パケットサイズが、MTU (Maximum Transmission Unit ; 伝送路の最大転送サイズ) に等しくなるようパディング処理を行う。ここで、MTUは、最大伝送量探索部105から受け取る情報である。

5 また、通信部101は、ルータ11から暗号化されたIPペイロードを含む受信用パケットを受信し、受信した受信用パケットを順次暗号処理部102に出力する。受信用パケットの具体例は、図4(a)に示したコンテンツサーバ検索パケット301、同図(c)に示した鍵共有要求パケット303などである。また、通信部101は、ルータ11から暗号化されたIPペイロードを含む受信用パケットを受信して蓄積し、受信情報を生成する。通信部101は、生成した受信情報を暗号処理
10 部102へ出力する。受信情報の具体例は、端末の公開鍵等である。

なお、コンテンツサーバ検索パケット301、確認パケット302及び鍵共有要求パケット303の具体的なデータ構造等については後述する。

(2) 暗号処理部102

15 暗号処理部102は、確認情報生成部107から、順次確認パケットを受け取り、受け取った確認パケットのIPペイロードを暗号化した後、通信部101へ出力する。暗号処理部102は、共有鍵生成部108からコンテンツサーバ20の公開鍵を受け取り、受け取った公開鍵を暗号化した後、通信部101へ出力する。

20 また、暗号処理部102は、通信部101からコンテンツサーバ検索パケットを順次受け取り、受け取ったコンテンツサーバ検索パケットのIPペイロードを復号したのち、AD判定部106へ出力する。暗号処理部102は、通信部101から鍵共有要求パケットを順次受け取り、受け取った鍵共有要求パケットのIPペイロードを復号してAD判定部106へ出力する。

25 このとき暗号処理部102が行う暗号化及び復号処理のアルゴリズムの一例は、秘密鍵暗号方式AES (Advanced Encryption Standard) であり、ここで用いる鍵情報は、予め、通信を行う機器との間で共有しているものとする。また、鍵情報は耐タンパ性領域に格納されているものとする。なお、AESについては、FIPS (Federal Information Processing Standard) - 197で定義されているため説明を省略する。

更に、暗号処理部102は、コンテンツ格納部109からコンテンツを受け取り、

共有鍵生成部 108 に格納されている共有鍵を読み出す。暗号処理部 102 は、読み出した共有鍵を用いてコンテンツを暗号化し、暗号化コンテンツを生成する。暗号処理部 102 は、生成した暗号化コンテンツを通信部 101 へ出力する。このとき暗号処理部 102 が行う暗号化処理のアルゴリズムの一例は、AES である。

5 (3) 機器 ID 管理部 103

機器 ID 管理部 103 は、コンテンツサーバ 20 を一意に識別するために用いられる機器 ID 「ID_A」を格納している。「ID_B」は、具体的には、コンテンツサーバ 20 に固有の 8 バイトデータである。

 (4) 中継機器固有情報取得部 104

10 中継機器固有情報取得部 104 は、コンテンツサーバ 20 が接続されているルータの MAC アドレスを取得して、内部の記憶領域に格納する。なお、中継機器固有
15 情報取得部 104 は、コンテンツサーバ 20 が初めてルータに接続されたとき、上記の処理を行うように構成してもよいし、また、定期的にコンテンツサーバ 20 が
15 接続されているルータの MAC アドレスを取得し、記憶領域に格納されている MAC
15 アドレスに上書きするように構成してもよい。

 なお、MAC アドレスの取得方法の一例は、ARP (Address Resolution Protocol) である。ARP については、RFC (Request For Comment) 825 で説明されているため、説明を省略する。

 (5) 最大伝送量探査部 105

20 最大伝送量探査部 105 は、コンテンツサーバ 20 が接続されているネットワークの最大伝送量を取得して、取得した最大伝送量を内部の記憶領域に格納する。なお、最大伝送量探査部 105 は、コンテンツサーバ 20 が初めてネットワークに接続されたとき 1 回のみ上記処理を行うように構成してもよいし、定期的にコンテンツサーバ 20 が接続されているネットワークの最大伝送量を取得し、記憶領域に格納されている最大伝送量に上書きするように構成してもよい。

 なお、最大伝送量の取得方法としては、RFC 1191 で説明されている経路 MTU 探索の方法を用いる。

 (6) AD 判定部 106

 AD 判定部 106 は、他の機器からコンテンツの要求を受けて、当該他の機器が

AD内の機器であるか否かを判定する。

AD判定部106は、コンテンツサーバ20が初めてネットワークに接続されたときインターネット60を介して、発行機関からCRL(Certification Revocation List)を受信し、記憶する。CRLは、秘密鍵が暴露された機器など、無効化された機器の機器IDが登録されているリストである。AD判定部106は、インターネット60を介して、発行機関から常に最新のCRLを受信し、それまで記憶していたCRLに上書きする。

AD判定部106は、暗号処理部102から、コンテンツサーバ検索パケットを受け取ったとき、及び、鍵共有要求パケットを受け取ったとき、以下の(判断1)から(判断3)までの処理を行う。

(判断1) AD判定部106は、コンテンツサーバ検索パケット及び鍵共有要求パケットから機器IDを読み出し、読み出した機器IDが、内部に記憶しているCRLに記載されておらず、送信元端末が無効化されていないか否か判断する。

(判断2) 次に、AD判定部106は、コンテンツサーバ検索パケット及び鍵共有要求パケットからTTLを読み出し、読み出したTTLが「1」であるか否か判断する。

(判断3) 次に、AD判定部106は、コンテンツサーバ検索パケット及び鍵共有要求パケットから中継機器固有情報を読み出す。また、AD判定部106は、中継機器固有情報取得部104が記憶している中継機器固有情報を読み出す。AD判定部106は、読み出した2個の中継機器固有情報が同一であるか否か判断する。

コンテンツサーバ検索情報に対する上記1、2、及び3の判断において、全てが肯定的である場合に、AD判定部106は、当該コンテンツサーバ検索パケットを送信した端末へ送信する確認パケットを生成する指示を、確認情報生成部107へ出力する。

鍵共有要求パケットに対する上記1、2及び3の判断において、全てが肯定的である場合に、AD判定部106は、当該鍵共有要求パケットを送信した端末との間で共有鍵を生成する指示を、共有鍵生成部108へ出力する。

ここで、「TTL (Time To Live)」は、ネットワーク上に送出されたパケットが、ルータの設定ミスなどによりループになってしまった場合に、パケットがネ

ネットワーク上に生存し続けることを防ぐため、パケットの生存可能時間を表すものである。具体的には、ホップカウントをもってTTLとする。端末は、パケット送信時に、所定のTTLをIPヘッダのTTLフィールドに設定する。設定されたTTLは、パケットがルータを通過して次の中継機器であるルータに送出される毎に1ずつデクリメントされる。TTLが0になるとパケットはルータによって破棄され、それ以上転送されない。

(7) 確認情報生成部107

確認情報生成部107は、AD判定部106からの指示を受けて、以下に示す様に確認パケットを生成する。確認パケットは、IPヘッダとIPペイロードとから構成される。以下では、図4(b)に示した確認パケット302を例に説明する。

IPヘッダは、DF(Don't Fragment)ビット、TTL、及び宛先アドレスを含む。DFビットは、「有効」又は「無効」の何れかに設定される。「有効」はフラグメントが禁止されていることを示し、「無効」はフラグメントが許可されていることを示す。フラグメントとは、パケットを分割して送信する機能である。図4(b)に示す様に、確認情報生成部107は、DFビットを「有効」に設定し、フラグメントを禁止することで、所謂「カプセル化」を抑止する。確認情報生成部107は、TTLを「1」に設定し、確認パケット302が、ルータ11を越えて他のネットワークへ送出されることを抑止する。確認情報生成部107は、コンテンツサーバ検索パケットを送信した送信元端末のIPアドレスを、宛先アドレスとする。送信元端末のIPアドレスは、送信元端末の機器IDと対応付けて、予め確認情報生成部107が記憶していてもよいし、送信元端末から送信されるパケットに含まれており、確認情報生成部107がパケットからIPアドレスを抽出するように構成されてもよい。

IPペイロードは、パケット種別、コンテンツサーバアドレス、中継機器固有情報及びパディングデータを含む。確認情報生成部107は、当該パケットが確認パケットであることを示す為に、パケット種別として「確認」を書き込む。確認情報生成部107は、コンテンツサーバアドレスとして、自身のIPアドレスを書き込む。確認情報生成部107は、中継機器固有情報取得部104からルータのMACアドレスを読み出し、読み出したMACアドレスを、中継機器固有情報として書き込む。

確認情報生成部107は、確認パケット302のデータサイズがMTUに等しくなるよう、パディングデータを書き込む。ここでは、例としてパディングデータは「0」である。

5 確認情報生成部107は、上記の様に生成した確認パケット302を、順次暗号処理部102へ出力する。

(8) 共有鍵生成部108

共有鍵生成部108は、予め、外部の管理センタから楕円曲線 $E: y = x^3 + ax + b$ と元 G とが与えられているものとする。

10 共有鍵生成部108は、AD判定部106から、鍵共有要求パケットを送信した端末との間で共有鍵を生成する指示を受け取ると、以下に示す様にして、共有鍵生成処理を行う。

共有鍵生成部108は、秘密鍵 x_A を設定して次式により公開鍵 Y_A を算出する。

$$Y_A = x_A * G$$

15 共有鍵生成部108は、算出した公開鍵 Y_A を、送信元端末へ送信すると共に、送信元端末から、送信元端末の公開鍵 Y_B を受信する。

共有鍵生成部108は、受信した送信元端末の公開鍵 Y_B と自身の秘密鍵とから、 $x_A * Y_B$ を算出することにより共有鍵を生成し、生成した共有を内部に記憶する。

共有鍵生成部108は、共有鍵を生成して記憶すると、コンテンツ格納部109に対して、コンテンツを読み出す指示を出力する。

20 (9) コンテンツ格納部109

コンテンツ格納部109は、具体的にはハードディスクドライブユニットであって、内部にコンテンツを格納している。共有鍵生成部108からの指示を受けて、読み出したコンテンツを暗号処理部102へ出力する。

2. 端末30の構成

25 端末30は、ルータ11に接続されたAD内の機器であり、ルータ11を介してコンテンツサーバ20との間で鍵共有処理を行い、共有鍵を用いてコンテンツの送受信を行う。

図3は、端末30の構成を機能的に示す機能ブロック図である。同図に示す様に、端末30は、通信部201、暗号処理部202、機器ID管理部203、中継機器

固有情報取得部 204、最大伝送量探査部 205、コンテンツサーバ検索情報生成部 206、鍵共有要求情報生成部 207、共有鍵生成部 208 及び記憶部 209 から構成され

5 端末 30 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ネットワーク接続ユニット、ディスプレイユニット、リモートコントローラなどから構成され、より具体的には、端末 30 は、ネットワークに接続可能な AV 機器や家電製品などである。前記 RAM 又は前記ハードディスクユニットにはコンピュータプログラムが記憶されており、前記マイクロプロセッサが、前記コンピュータプログラムに従い動作することにより、端末 30 は、各種の機能を達成
10 する。

(1) 通信部 201

通信部 201 は、ルータ 11 を介して IP パケットを送受信することにより他の機器と通信を行う通信インターフェースである。

15 通信部 201 は、暗号処理部 202 により IP ペイロードが暗号化された送信用パケットを順次受け取り、受け取った送信用パケットをルータ 11 へ送出する。送信用パケットの具体例は、図 4 (a) に示したコンテンツサーバ検索パケット 301、同図 (c) に示した鍵共有要求パケット 303 等である。また、通信部 201 は、暗号処理部 202 により暗号化された送信情報を受け取り、受け取った送信情報を分割して送信用パケットを生成し、生成した送信用パケットを順次ルータ 11
20 へ送出する。送信情報の具体例は、端末 30 の公開鍵等である。なお、通信部 201 は、送信情報を分割して送信用パケットを生成する際、パケットサイズが、MTU に等しくなるようパディング処理を行う。ここで、MTU は、最大伝送量探査部 205 から受け取る情報である。

25 また、通信部 201 は、ルータ 11 から暗号化された IP ペイロードを含む受信用パケットを受信し、受信した受信用パケットを順次暗号処理部 202 に出力する。受信用パケットの具体例は、図 4 (b) に示した確認パケット 302 などである。また、通信部 201 は、ルータ 11 から暗号化された IP ペイロードを含む受信用パケットを受信して蓄積し、受信情報を生成する。通信部 201 は、生成した受信情報を暗号処理部 202 へ出力する。受信情報の具体例は、暗号化コンテンツなど

である。

(2) 暗号処理部 202

暗号処理部 202 は、コンテンツサーバ 20 の暗号処理部 102 と同様の構成及び機能を有する。

5 暗号処理部 202 は、コンテンツサーバ検索情報生成部 206 から、順次コンテンツサーバ検索パケットを受け取り、受け取ったコンテンツサーバ検索パケットの IP ペイロードを暗号化した後、通信部 201 へ出力する。同様に、暗号処理部 202 は、鍵共有要求情報生成部 207 から鍵共有要求パケットを受け取り、受け取った鍵共有要求パケットの IP ペイロードを暗号化した後、通信部 201 へ出力する。また、暗号処理部 202 は、共有鍵生成部 208 から端末 30 の公開鍵を受け取り、受け取った公開鍵を暗号化した後、通信部 201 へ出力する。

また、暗号処理部 202 は、通信部 201 から確認パケットを順次受け取り、受け取った確認パケットの IP ペイロードを復号したのち、鍵共有要求情報生成部 207 へ出力する。

15 このとき暗号処理部 202 が行う暗号化及び復号処理のアルゴリズムの一例は、秘密鍵暗号方式 AES であり、ここで用いる鍵情報は、予め、コンテンツサーバ 20 との間で共有しているものとする。また、鍵情報は耐タンパ性領域に格納されているものとする。

20 更に、暗号処理部 202 は、通信部 201 から暗号化コンテンツを受け取り、共有鍵生成部 208 に格納されている共有鍵を読み出す。暗号処理部 202 は、読み出した共有鍵を用いて暗号化コンテンツを復号し、コンテンツを生成する。暗号処理部 202 は、生成したコンテンツを記憶部 209 に格納する。

(3) 機器 ID 管理部 203

25 機器 ID 管理部 203 は、端末 30 を一意に識別するために用いられる機器 ID 「ID_B」を格納している。「ID_B」は、具体的に、端末 30 に固有の 8 バイトデータである。

(4) 中継機器固有情報取得部 204

中継機器固有情報取得部 204 は、端末 30 が接続されているルータの MAC アドレスを取得して、内部の記憶領域に格納する。なお、中継機器固有情報取得部 2

04は、端末30が初めてルータに接続されたとき、上記の処理を行うように構成してもよいし、また、定期的に端末30が接続されているルータのMACアドレスを取得し、記憶領域に格納されているMACアドレスに上書きするように構成してもよい。なお、MACアドレスの取得方法の一例は、ARPである。

5 (5) 最大伝送量探査部205

最大伝送量探査部205は、端末30が接続されているネットワークの最大伝送量を取得して、取得した最大伝送量を内部の記憶領域に格納する。なお、最大伝送量探査部205は、端末30が初めてネットワークに接続されたとき1回のみ上記の処理を行うように構成してもよいし、定期的に端末30が接続されているネットワークの最大伝送量を取得し、記憶領域に格納されている最大伝送量に上書きするように構成してもよい。

なお、最大伝送量の取得方法としては、RFC1191で説明されている経路MTU探索の方法を用いる。

(6) コンテンツサーバ検索情報生成部206

15 コンテンツサーバ検索情報生成部206は、要求が発生すると、以下に示す様にコンテンツサーバ検索パケットを生成する。コンテンツサーバ検索パケットは、IPヘッダとIPペイロードとから構成される。以下では、図4(a)に示したコンテンツサーバ検索パケット301を例に説明する。

20 IPヘッダは、DFビット、TTL、及び宛先アドレスを含み、コンテンツサーバ検索情報生成部206は、DFビットを「有効」に設定し、フラグメントを禁止する。コンテンツサーバ検索情報生成部206は、TTLを「1」に設定する。また、コンテンツサーバ検索情報生成部206は、マルチキャストアドレスを宛先アドレスとする。なお、コンテンツサーバ検索情報生成部206が設定するTTLは、予めコンテンツサーバ20から通知されているものとする。

25 IPペイロードは、パケット種別、機器ID、中継機器固有情報及びパディングデータを含む。コンテンツサーバ検索情報生成部206は、当該パケットがコンテンツサーバ検索パケットであることを示す為に、パケット種別として「コンテンツサーバ検索」を書き込む。コンテンツサーバ検索情報生成部206は、機器IDとして、機器ID管理部203から「ID_B」を読み出し、読み出した「ID_B」

を書き込む。コンテンツサーバ検索情報生成部206は、中継機器固有情報取得部204からルータのMACアドレスを読み出し、読み出したMACアドレスを、中継機器固有情報として書き込む。コンテンツサーバ検索情報生成部206は、コンテンツサーバ検索パケット301のデータサイズがMTUに等しくなるよう、パディングデータを書き込む。ここでは、例としてパディングデータは「0」である。

コンテンツサーバ検索情報生成部206は、上記の様に生成したコンテンツサーバ検索パケット301を、順次暗号処理部202へ出力する。

(7) 鍵共有要求情報生成部207

鍵共有要求情報生成部207は、暗号処理部202から、確認パケットを受け取ると、以下に示す様に鍵共有要求パケットを生成する。鍵共有要求パケットは、IPヘッダとIPペイロードとから構成される。以下では、暗号処理部202から、図4(b)に示した確認パケット302を受け取り、図4(c)に示した鍵共有要求パケット303を生成する例に基づき説明する。

IPヘッダは、DFビット、TTL及び宛先アドレスを含む。鍵共有要求情報生成部207は、DFビットを「有効」に設定する。鍵共有要求情報生成部207は、TTLを「1」に設定する。鍵共有要求情報生成部207は、宛先アドレスとして、確認パケット302のIPペイロードからコンテンツサーバ20のIPアドレスを読み出し、当該IPアドレスを書き込む。なお、鍵共有要求情報生成部207が設定するTTLは、予めコンテンツサーバ20から通知されているものとする。

IPペイロードは、パケット種別、機器ID、中継機器固有情報及びパディングデータを含む。鍵共有要求情報生成部207は、当該パケットが、鍵共有要求パケットであることを示すために、パケット種別として「鍵共有要求」を書き込む。鍵共有要求情報生成部207は、機器IDとして、機器ID管理部203から、「ID_B」を読み出し、読み出した「ID_B」を書き込む。鍵共有要求情報生成部207は、中継機器固有情報取得部204からルータのMACアドレスを読み出し、読み出したMACアドレスを、中継機器固有情報として書き込む。鍵共有要求情報生成部207は、鍵共有要求パケット303のデータサイズがMTUに等しくなるよう、パディングデータを書き込む。ここでは、例としてパディングデータは「0」である。

鍵共有要求情報生成部207は、上記の様に生成した鍵共有要求パケット303を、順次暗号処理部202へ出力する。

(8) 共有鍵生成部208

5 共有鍵生成部208は、予め、外部の管理センタから楕円曲線Eと元Gとが与えられているものとする。

共有鍵生成部208は、鍵共有要求情報生成部207により、鍵共有要求パケットが生成され、鍵共有要求パケットが、コンテンツサーバ20へ送信されると、以下に示す様にして、共有鍵生成処理を行う。

10 共有鍵生成部208は、秘密鍵 x_B を設定して、次式により公開鍵 Y_B を算出する。

$$Y_B = x_B * G$$

共有鍵生成部208は、算出した公開鍵 Y_B を、コンテンツサーバ20へ送信すると共に、コンテンツサーバ20から、コンテンツサーバ20の公開鍵である Y_A を受信する。

15 共有鍵生成部208は、自身の秘密鍵と受信したコンテンツサーバ20の公開鍵 Y_A とから、 $x_B * Y_A$ を算出することにより共有鍵を生成し、生成した共有鍵を内部に記憶する。

ここで、先程、コンテンツサーバ20の共有鍵生成部108により算出された共有鍵 $x_A * Y_B$ は、

20
$$x_A * Y_B = (x_A \times x_B) * G$$

のように変形できる。

一方、共有鍵生成部208により算出された共有鍵 $x_B * Y_A$ は、

$$\begin{aligned} x_B * Y_A &= (x_B \times x_A) * G \\ &= (x_A \times x_B) * G \end{aligned}$$

25 のように変形できる。

従って、共有鍵生成部108により算出された共有鍵 $x_A * Y_B$ と、共有鍵生成部208により算出された共有鍵 $x_B * Y_A$ とが同じものであることは明らかである。

(9) 記憶部209

記憶部209は、具体的にはハードディスクドライブユニットであり、暗号処理部202により復号されたコンテンツを受け取り、受け取ったコンテンツを格納する。

3. 端末40及び端末50の構成

5 端末40及び端末50は、図1に示す様に、ルータ12の下に接続された機器である。端末40及び端末50は、通信部、暗号処理部、機器ID管理部、中継機器固有情報取得部、最大伝送量探査部、コンテンツサーバ検索情報生成部、鍵共有要求情報生成部、共有鍵生成部及び記憶部から構成される。

10 端末40及び端末50の構成は、端末30と同一であり、各構成要素の機能も端末30の各構成要素と同一であるため、端末40及び端末50の機能ブロック図は図示しておらず、説明を省略する。

端末40及び端末50は、TTLを「1」に設定したコンテンツサーバ検索パケットを送信すると、コンテンツサーバ検索パケットは、ルータ12で破棄され、コンテンツサーバ20へは到達しない。

15 ここで、例えば、端末40及び端末50が、TTLを「4」に設定した不正なコンテンツサーバ検索パケットを送出すると、当該コンテンツサーバ検索パケットは、コンテンツサーバ20へ到達する。しかしながら、コンテンツサーバ20は、コンテンツサーバ検索パケットを受信すると、TTLを「1」に設定した確認パケットを送信元端末へ返送するため、結局、当該確認パケットは、端末40及び端末50
20 には到達せず、端末40及び端末50は、コンテンツサーバ20のIPアドレスを取得することは出来ない。ゆえに、端末40及び端末50は、コンテンツサーバ20と鍵共有処理を行うことが出来ない。

<動作>

ここでは、図5から図9に示したフローチャートを用いて、コンテンツ配信システム1の動作について説明する。
25

(1) 全体の動作

先ず、図5に示したフローチャートを用いて、コンテンツ配信システム1全体の動作について説明する。

端末30において要求が発生すると（ステップS1）、コンテンツサーバ20及

び端末30の間でAD判定処理を行う（ステップS2）。続いて、コンテンツサーバ20及び端末30の間で鍵共有処理を行い（ステップS3）、コンテンツサーバ20は、コンテンツ送信処理を行い（ステップS4）、端末30は、コンテンツ受信処理を行う（ステップS5）。

5 なお、図5のフローチャートは、コンテンツサーバ20及び端末30の動作のみを記載しているが、端末40及び端末50は、端末30と同様に動作するため、ここでは、説明の便宜上、コンテンツサーバ20及び端末30の動作のみを記載している。

（2）AD判定処理の動作

10 ここでは、図6及び図7に示したフローチャートを用いて、AD判定処理の動作について説明する。なお、ここで説明する動作は、図5のステップS2の詳細である。

15 端末30の中継機器固有情報取得部204は、自身が接続されているルータのMACアドレスを取得する（ステップS11）。コンテンツサーバ検索情報生成部206は、TTLを「1」に設定し、中継機器固有情報として、ステップS11で取得したMACアドレスを書き込み、MTUに等しいデータサイズのコンテンツサーバ検索パケットを生成する（ステップS12）。コンテンツサーバ検索情報生成部206は、生成したコンテンツサーバ検索パケットを、順次暗号処理部202へ出力し、暗号処理部202は、コンテンツサーバ検索パケットを受け取り、受け取ったパケットのIPペイロードを暗号化する（ステップS13）。通信部201は、IPペイロードが暗号化されたコンテンツサーバ検索パケットを、マルチキャスト送信する（ステップS14）。

20 コンテンツサーバ20は、端末30から送信されたコンテンツサーバ検索パケットを受信し（ステップS14）、暗号化されているIPペイロードを、暗号処理部102により復号する（ステップS15）。AD判定部106は、コンテンツサーバ検索パケットのIPペイロードに含まれる送信元端末（端末30）の機器IDを読む（ステップS16）。AD判定部106は、内部に格納しているCRLを参照し、端末30の機器IDが、CRLに記載されているか否か判断し、機器IDがCRLに記載されている場合（ステップS17でYES）、コンテンツサーバ20は

処理を終了する。

機器IDがCRLに記載されていない場合（ステップS17でNO）、AD判定部106は、IPヘッダに含まれるTTLを読む（ステップS18）。TTLが「1」でない場合（ステップS19でNO）、コンテンツサーバ20は処理を終了する。

5 TTLが「1」の場合（ステップS19でYES）、AD判定部106は、IPペイロードに含まれる中継機器固有情報と、中継機器固有情報取得部104が記憶している中継機器固有情報とを取得する（ステップS20）。AD判定部106は、両者が一致するか否か判断し、一致しない場合（ステップS21でNO）、コンテンツサーバ20は処理を終了する。

10 一致する場合（ステップS21でYES）、AD判定部106は、確認情報生成部107に確認パケットを生成する指示を出力し、確認情報生成部107は、TTLを「1」に設定し、自身のIPアドレスを含む確認パケットを生成し（ステップS22）、生成した確認パケットを暗号処理部102へ出力する。暗号処理部102は、確認パケットのIPペイロードを暗号化し（ステップS23）、通信部101は、確認パケットを端末30へ送信し、端末30は、確認パケットを受信する（ステップS24）。

15 端末30の暗号処理部202は、受信した確認パケットのIPペイロードを復号し（ステップS25）、確認パケットを鍵共有要求情報生成部207へ出力する。鍵共有要求情報生成部207は、確認パケットのIPペイロードに含まれるコンテンツサーバ20のIPアドレスを宛先アドレスとし、TTLを「1」に設定し、中継機器固有情報を書き込み、パケットのデータサイズをMTUに設定して鍵共有要求パケットを生成する（ステップS26）。

20 鍵共有要求情報生成部207は、生成した鍵共有要求パケットを暗号処理部202へ出力し、暗号処理部202は、鍵共有要求パケットのIPペイロードを暗号化する（ステップS27）。通信部201は、鍵共有要求パケットをコンテンツサーバ20へ送信し、コンテンツサーバ20は、鍵共有要求パケットを受信する（ステップS28）。

25 コンテンツサーバ20の暗号処理部102は、受信した鍵共有要求パケットのIPペイロードを復号し（ステップS29）、鍵共有要求パケットをAD判定部10

6へ出力する。AD判定部106は、鍵共有要求パケットのIPペイロードに含まれる端末30の機器IDを読む(ステップS30)。AD判定部106は、内部に格納しているCRLを参照し、ステップS30で読み出した端末30の機器IDが、CRLに記載されているか否か判断し、機器IDがCRLに記載されている場合(ステップS31でYES)、コンテンツサーバ20は処理を終了する。

機器IDがCRLに記載されていない場合(ステップS31でNO)、AD判定部106は、IPヘッダに含まれるTTLを読む(ステップS32)。TTLが「1」でない場合(ステップS33でNO)、コンテンツサーバ20は処理を終了する。

TTLが「1」の場合(ステップS33でYES)、AD判定部106は、IPペイロードに含まれる中継機器固有情報と、中継機器固有情報取得部104が記憶している中継機器固有情報とを取得する(ステップS34)。AD判定部106は、両者が一致するか否か判断し、一致しない場合(ステップS35でNO)、コンテンツサーバ20は処理を終了する。一致する場合(ステップS35でYES)、コンテンツサーバ20及び端末30は、図5のステップS3の処理を続ける。

(3) 鍵共有処理の動作

ここでは、図8に示したフローチャートを用いて、鍵共有処理の動作について説明する。なお、ここで説明する動作は、図5のステップS3の詳細であり、コンテンツサーバ20の共有鍵生成部108及び端末30の共有鍵生成部208で行われる処理である。

コンテンツサーバ20は、秘密鍵 x_A を設定し(ステップS41)、一方で、端末30は、秘密鍵 x_B を設定する(ステップS42)。

コンテンツサーバ20及び端末30は、共に管理センタから、楕円曲線 $E: y = x^3 + ax + b$ と、元 G とを取得する(ステップS43及びステップS44)。

コンテンツサーバ20は、公開鍵 $Y_A = x_A * G$ を算出し(ステップS45)、算出した公開鍵 Y_A を端末30へ送信し、端末30はコンテンツサーバ20の公開鍵 Y_A を受信する(ステップS47)。

一方、端末30は、公開鍵 $Y_B = x_B * G$ を算出し(ステップS46)、算出した公開鍵 Y_B をコンテンツサーバ20へ送信し、コンテンツサーバ20は、端末30の公開鍵 Y_B を受信する(ステップS48)。

コンテンツサーバ20は、共有鍵 $x_A * Y_B$ を算出し（ステップS49）、端末30は、共有鍵 $x_B * Y_A$ を算出する（ステップS50）。

このとき、コンテンツサーバ20が算出する共有鍵は、

$$x_A * Y_B = (x_A \times x_B) * G \text{ と変形できる。}$$

5 一方、端末30が算出する共有鍵は、

$$x_B * Y_A = (x_B \times x_A) * G$$

$$= (x_A \times x_B) * G \text{ と変形できる。}$$

従って、コンテンツサーバ20と端末30とで算出された共有鍵は同一のものであることがわかる。

10 コンテンツサーバ20の共有鍵生成部108、及び、端末30の共有鍵生成部208は、それぞれ、算出した共有鍵を内部に格納する。続いて、コンテンツサーバ20は、図5のステップS4の処理を続け、端末30はステップS5の処理を続ける。

(4) コンテンツ送信処理の動作

15 ここでは、図9(a)に示したフローチャートを用いてコンテンツ送信処理の動作について説明する。なお、ここで説明する動作は、図5のステップS4の詳細である。

共有鍵生成部108からの指示を受け、コンテンツ格納部109は、内部に格納しているコンテンツを読み出し（ステップS61）、読み出したコンテンツを暗号処理部102へ出力する。暗号処理部102は、コンテンツを受け取ると、共有鍵生成部108から共有鍵「 $x_A * Y_B$ 」を読み出す（ステップS62）。

暗号処理部102は、共有鍵「 $x_A * Y_B$ 」を暗号鍵として用いてコンテンツを暗号化し、暗号化コンテンツを生成する（ステップS63）。

25 通信部101は、暗号化コンテンツを、端末30へ送信し（ステップS64）、図5のフローチャートに戻る。

(5) コンテンツ受信処理の動作

ここでは、図9(b)に示したフローチャートを用いてコンテンツ受信処理の動作について説明する。なお、ここで説明する動作は、図5のステップS5の詳細である。

端末30の通信部201は、コンテンツサーバ20から暗号化コンテンツを受信する(ステップS71)。通信部201は、受信した暗号化コンテンツを暗号処理部202へ出力する。

5 暗号処理部202は、暗号化コンテンツを受け取ると、共有鍵生成部208が記憶している共有鍵「 $x B * Y A$ 」を読み出す(ステップS72)。

暗号処理部202は、共有鍵「 $x B * Y A$ 」を復号鍵として用い暗号化コンテンツを復号してコンテンツを生成する(ステップS73)。暗号処理部202は、復号したコンテンツを記憶部209へ格納し(ステップS74)、図5のフローチャートに戻る。

10 <変形例1>

ここでは、コンテンツ配信システム1の第1変形例であるコンテンツ配信システム1aについて説明する。コンテンツ配信システム1において、AD内には一つのルータが存在し、AD内の各機器は、当該一つのルータ下に接続されていた。これに対し、コンテンツ配信システム1aにおいては、AD内には複数のルータが存在し、AD内の各機器は、複数のルータを介してコンテンツサーバ20と接続されている。

以下では、図面を参照して詳細に説明する。

20 図10は、コンテンツ配信システム1aの構成を示す図である。同図に示す様に、コンテンツ配信システム1aは、ルータ10、ルータ11、ルータ11a、ルータ11b、ルータ12、コンテンツサーバ20、端末30a及び端末30bから構成される。インターネット60に接続されたルータ10には、ルータ11及びルータ12が接続されている。ルータ11、ルータ11a及びルータ11bは、AD内に存在する中継機器であり、ルータ12は、AD外に存在する中継機器である。

25 ルータ11には、コンテンツサーバ20とルータ11aとが接続されており、ルータ11aには、端末30aとルータ11bとが接続されており、ルータ11bには端末30bが接続されている。ルータ12には、1以上の端末が接続されているが、ルータ12に接続されている端末については図示しておらず説明を省略する。

なお、コンテンツ配信システム1aにおいて、各機器は通信プロトコルとしてIPv4を使用して通信を行うものとする。

ここで、コンテンツサーバ20は、第1の実施の形態におけるコンテンツサーバ20と同一の構成及び機能を有するため説明を省略する。

図11は、端末30bの構成を機能的に示す機能ブロック図である。同図に示す様に、端末30bは、通信部201、暗号処理部202、機器ID管理部203、
5 最大伝送量探査部205、TTL検索部206b、鍵共有要求情報生成部207、共有鍵生成部208及び記憶部209から構成される。図11において、端末30(図3)と同一の機能を有する構成要素には、図3で用いた符号と同一の符号を付し、説明を省略する。

端末30bは、端末30と異なり、中継機器固有情報取得部204とコンテンツ
10 サーバ検索情報生成部206とを有しておらず、TTL検索部206bを有する。端末30bは、コンテンツサーバ20と通信を行うために設定すべきTTLを知る必要があり、TTL検索部206bは、適切なTTLを検索する機能を有する。

TTL検索部206bは、図12に示すTTL検索パケット304を生成する。同図に示す様に、TTL検索パケット304は、IPヘッダとIPペイロードとから構成され、IPヘッダは、DFビット「有効」、TTL「n」及び宛先アドレス「マルチキャストアドレス」を含み、IPペイロードは、パケット種別「TTL検索」、機器ID「ID_C」及びパディングデータ「0」を含む。ここで、「n」は、 $1 \leq n < 255$ を満たす整数である。また、「ID_C」は、端末30bを一
15 意に識別する機器IDであり、具体的には機器ID管理部203に記憶されている
20 端末30bに固有の8バイトデータである。なお、端末30aは、端末30bと同様の構成及び機能を有するため説明を省略する。

図13は、コンテンツ配信システム1a全体の動作を示すフローチャートである。

端末30bにおいて要求が発生すると(ステップS81)、端末30bは、TTL
L検索処理を行い(ステップS82)、コンテンツサーバ20と通信を行うために
25 設定すべきTTLを検索する。TTLが決定すると、コンテンツサーバ20及び端
末30bの間でAD判定処理を行う(ステップS83)。続いて、コンテンツサ
ーバ20及び端末30bの間で鍵共有処理を行い(ステップS84)、コンテンツサ
ーバ20は、コンテンツ送信処理を行い(ステップS85)、端末30bは、コン
テンツ受信処理を行う(ステップS5)。

なお、図13のフローチャートは、コンテンツサーバ20及び端末30bの動作のみを記載しているが、端末30aは、端末30bと同様に動作するため、ここでは、説明の便宜上コンテンツサーバ20及び端末30bの動作のみを記載している。

次に、図14に示したフローチャートを用いて、端末30bがコンテンツサーバ20と通信を行うために設定すべきTTLを検索する処理の動作について説明する。
5 なお、ここで説明する動作は、図13に示したフローチャートのステップS82の詳細である。

TTL検索部206bは、先ず、nとして1を設定する（ステップS91）。TTL検索部206bは、TTL検索パケットのTTLを「n」に設定し、TTL検索
10 パケットを生成する。暗号処理部202は、生成されたTTL検索パケットのIPペイロードを暗号化して、通信部201は、TTL検索パケットをマルチキャスト送信する（ステップS92）。

TTL検索部206bは、コンテンツサーバ20から確認パケットを受信した場合（ステップS93でYES）、コンテンツサーバ20との通信に用いるTTLを
15 「n」に決定し（ステップS94）、処理を終了する。

TTL検索部206bは、コンテンツサーバ20から確認パケットを受信しない場合（ステップS93でNO）、nが255より小さい数であるか否か判断する。nが255以上である場合（ステップS95でNO）には、TTL検索部206bは、コンテンツサーバ20の検索に失敗したとみなし処理を終了する。

20 nが255より小さい場合（ステップS95でYES）、TTL検索部206bは、 $n = n + 1$ とし（ステップS96）、ステップS82に戻り処理を続ける。

この様にして、端末30bは、コンテンツサーバ20からの応答があるまで、TTL検索パケットのTTLを1から255まで1ずつインクリメントしてTTL検索パケットを生成し、マルチキャスト送信を続ける。

25 続いて、図15及び図16に示すフローチャートを用いて、AD判定処理の動作について説明する。なお、ここで説明する動作は、図13に示したフローチャートのステップS83の詳細である。

端末30bのTTL検索部206bは、TTL検索パケットを生成し（ステップS101）、暗号処理部202は、生成されたTTL検索パケットのIPペイロー

ドを暗号化する（ステップS102）。通信部201は、IPペイロードが暗号化されたTTL検索 packets をマルチキャスト送信し、コンテンツサーバ20の通信部101は、TTL検索 packets を受信する（ステップS103）。

5 暗号処理部102は、暗号化されているIPペイロードを復号する（ステップS104）。AD判定部106は、TTL検索 packets のIPペイロードに含まれる送信元端末（端末30b）の機器IDを読む（ステップS105）。AD判定部106は、内部に格納しているCRLを参照し、ステップS105で読み出した機器IDが、CRLに記載されているか否か判断し、機器IDがCRLに記載されている場合（ステップS106でYES）、コンテンツサーバ20は処理を終了する。

10 機器IDがCRLに記載されていない場合（ステップS106でNO）、AD判定部106は、確認情報生成部107に確認 packets を生成する指示を出力し、確認情報生成部107は、TTL検索 packets に含まれるTTLと等しいTTLをIPヘッダに設定し、自身のIPアドレスを含む確認 packets を生成し（ステップS109）、生成した確認 packets を暗号処理部102へ出力する。暗号処理部102は、確認 packets のIPペイロードを暗号化し（ステップS110）、通信部101は、確認 packets を端末30bへ送信し、端末30bは、確認 packets を受信する（ステップS111）。

20 端末30bの暗号処理部202は、受信した確認 packets のIPペイロードを復号し（ステップS112）、確認 packets を鍵共有要求情報生成部207へ出力する。鍵共有要求情報生成部207は、確認 packets のIPペイロードに含まれるコンテンツサーバ20のIPアドレスを宛先アドレスとし、ステップS94で決定したnをTTLに設定し、 packets のデータサイズをMTUに設定して鍵共有要求 packets を生成する（ステップS113）。

25 鍵共有要求情報生成部207は、生成した鍵共有要求 packets を暗号処理部202へ出力し、暗号処理部202は、鍵共有要求 packets のIPペイロードを暗号化する（ステップS114）。通信部201は、鍵共有要求 packets をコンテンツサーバ20へ送信し、コンテンツサーバ20は、鍵共有要求 packets を受信する（ステップS115）。

コンテンツサーバ20の暗号処理部102は、受信した鍵共有要求 packets のI

Pペイロードを復号し（ステップS116）、鍵共有要求パケットをAD判定部106へ出力する。AD判定部106は、鍵共有要求パケットのIPペイロードに含まれる端末30bの機器IDを読む（ステップ117）。AD判定部106は、内部に格納しているCRLを参照し、端末30bの機器IDが、CRLに記載されているか否か判断し、機器IDがCRLに記載されている場合（ステップS118でYES）、コンテンツサーバ20は処理を終了する。

機器IDがCRLに記載されていない場合（ステップS118でNO）、コンテンツサーバ20及び端末30bは、図13のステップS84の処理を続ける。

図13のステップS84の詳細は、図8に示したフローチャートと同一の処理であり、ステップS85の詳細は、図9（a）に示したフローチャートと同一の処理であり、ステップS86の詳細は、図9（b）に示したフローチャートと同一の処理であるため、説明を省略する。

<変形例2>

ここでは、コンテンツ配信システム1の第2変形例として、コンテンツ配信システム1bについて説明する。

コンテンツ配信システム1bは、AD判定処理の後に鍵共有処理を行うのではなく、鍵共有処理において各機器がTTLを「1」に設定したパケットを送受信することで、鍵共有処理とAD判定処理とを同時に行うシステムである。以下では、図面を参照して詳細に説明する。

図17は、コンテンツ配信システム1bの構成を示す図である。コンテンツ配信システム1bは、ルータ10、ルータ11、ルータ12、コンテンツサーバ20b、端末30c、端末40及び端末50から構成される。ルータ10、ルータ11、ルータ12、端末40及び端末50は、コンテンツ配信システム1（図1）と同一の構成及び機能を有するためコンテンツ配信システム1と同一の符号を付して説明を省略する。ここでは、コンテンツ配信システム1と異なる構成及び機能を有するコンテンツサーバ20b及び端末30cについて説明する。

図18は、コンテンツサーバ20bの構成を機能的に示す機能ブロック図である。同図に示す様に、コンテンツサーバ20bは、通信部101、暗号処理部102、機器ID管理部103、最大伝送量探査部105、AD判定部106b、共有鍵生

成部108b及びコンテンツ格納部109から構成される。なお、図18において、コンテンツサーバ20（図2）と同一の機能を有する構成要素には、同一の符号を付して説明を省略する。

5 AD判定部106bは、端末30cから受信する公開鍵パケットに含まれるTTLを読み、TTLが「1」であり、確かにAD内の端末から送信されたパケットであるか否かを判定する。端末30cから受信する公開鍵パケットについては後述する。

10 共有鍵生成部108bは、コンテンツサーバ20の共有鍵生成部108と同様に、予め、外部の管理センタから楕円曲線 $E: y = x^3 + ax + b$ と元Gとが与えられている。共有鍵生成部108bは、秘密鍵 x_A を設定して公開鍵 $Y_A = x_A * G$ を算出する。共有鍵生成部108bは、算出した公開鍵 Y_A を分割して公開鍵パケットを生成する。共有鍵生成部108bは、生成した公開鍵パケットを、暗号処理部102及び通信部101を介して順次端末30cへ送信する。

15 コンテンツサーバ20bが生成する公開鍵パケットの一例として、公開鍵パケット305のデータ構造を図20（a）に示す。同図に示す様に、公開鍵パケット305は、IPヘッダとIPペイロードとから構成され、IPヘッダは、DFビット「有効」、TTL「1」及び宛先アドレス「端末30c」を含み、IPペイロードは、パケット種別「公開鍵」、機器ID「ID_A」、公開鍵「 Y_A 」及びパディングデータ「0」を含む。

20 共有鍵生成部108bは、DFビットを「有効」に設定することにより、カプセル化を抑止し、TTLを「1」に設定することにより、公開鍵パケット305が、ルータ11を超えてAD外へ送信されることを抑止する。また、共有鍵生成部108bは、宛先アドレスに端末30cのIPアドレスを設定するが、当該IPアドレスは、コンテンツサーバ20bが既知であるとする。

25 同図に示す様に、公開鍵パケット305のデータサイズは、MTUに等しい。共有鍵生成部108bは、最大伝送量探査部105からMTUを取得し、取得したMTUに等しくなるようにパディング処理を施して、MTUに等しいデータサイズの公開鍵パケット305を生成する。また、公開鍵パケット305のIPペイロードは、暗号処理部102により暗号化されて、端末30cへ送信される。

共有鍵生成部108bは、端末30cから通信部101と暗号処理部102とを介して公開鍵パケットを受け取り、受け取った公開鍵パケットを蓄積して公開鍵YBを生成する。共有鍵生成部108bは、自身の秘密鍵xAと受信した端末30cの公開鍵YBとから、 $x A * Y B$ を算出することにより共有鍵 $x A * Y B$ を生成し、
5 生成した共有鍵 $x A * Y B$ を内部に記憶する。

共有鍵生成部108bは、共有鍵 $x A * Y B$ を生成して記憶すると、コンテンツ格納部109に対して、コンテンツを読み出す指示を出力する。

図19は、端末30cの構成を機能的に示す機能ブロック図である。同図に示す様に、端末30cは、通信部201、暗号処理部202、機器ID管理部203、
10 最大伝送量探査部205、共有鍵生成部208c及び記憶部209から構成される。

図19において、端末30（図3）と同一の機能を有する構成要素には、図3で用いた符号と同一の符号を付して説明を省略する。端末30cは、端末30と異なり、中継機器固有情報取得部204、コンテンツサーバ検索情報生成部205及び鍵共有要求情報生成部206を有していない。

15 共有鍵生成部208cは、端末30の共有鍵生成部208と同様に、予め、外部の管理センタから楕円曲線 $E: y = x^3 + a x + b$ と元Gとが与えられている。

共有鍵生成部208cは、秘密鍵xBを設定して、公開鍵 $Y B = x B * G$ を算出する。共有鍵生成部208cは、算出した公開鍵YBをパケットに分割して公開鍵パケットを生成し、生成した公開鍵パケットを、暗号処理部202及び通信部20
20 1を介して順次コンテンツサーバ20bに送信する。

端末30cが生成する公開鍵パケットの一例として、公開鍵パケット306のデータ構造を図20（b）に示す。同図に示す様に、公開鍵パケット306は、IPヘッダとIPペイロードとから構成され、IPヘッダは、DFビット「有効」、TTL「1」及び宛先アドレス「コンテンツサーバIPアドレス」を含み、IPペイ
25 ロードは、パケット種別「公開鍵」、機器ID「ID_M」、公開鍵「YB」及びパディングデータ「0」を含む。ここで、「ID_M」は、端末30cを一意に識別するために用いられる8バイトデータである。

共有鍵生成部208bは、DFビットを「有効」に設定することにより、カプセル化を抑止し、TTLを「1」に設定することにより、公開鍵パケット306が、

ルータ 11 を超えて A D 外へ送信されることを抑止する。また宛先アドレスとして設定するのはコンテンツサーバ 20 c の I P アドレスであり、当該 I P アドレスは予め端末 30 c が既知であるとする。

5 同図に示す様に、公開鍵パケット 306 のデータサイズは、MTU に等しい。共有鍵生成部 208 b は、最大伝送量探査部 205 から MTU を取得して、取得した MTU に等しいデータサイズにパディング処理を施して、公開鍵パケット 306 を生成する。また、公開鍵パケット 306 の I P ペイロードは、暗号処理部 202 により暗号化されて、コンテンツサーバ 20 b へ送信される。

10 共有鍵生成部 208 c は、コンテンツサーバ 20 b から通信部 201 と暗号処理部 202 とを介して公開鍵パケットを受け取り、受け取った公開鍵パケットを蓄積して公開鍵 Y A を生成する。

共有鍵生成部 208 は、自身の秘密鍵 x B と受信したコンテンツサーバ 20 b の公開鍵 Y A とから、 $x B * Y A$ を算出することにより共有鍵を生成し、生成した共有鍵 $x B * Y A$ を内部に記憶する。

15 次に、図 21 及び図 22 に示したフローチャートを用いて、コンテンツ配信システム 1 b の動作について説明する。

図 21 は、コンテンツ配信システム 1 b の全体の動作を示すフローチャートである。端末 30 c で要求が発生すると（ステップ S 201）、コンテンツサーバ 20 b と端末 30 c との間で鍵共有処理を行う（ステップ S 202）。続いて、コンテンツサーバ 20 b は、コンテンツ送信処理（ステップ S 203）を行い、端末 30 c は、コンテンツ受信処理を行う（ステップ S 204）。

図 22 は、鍵共有処理の動作を示すフローチャートである。なお、ここに示す動作は、図 21 に示したフローチャートのステップ S 202 の詳細である。

25 コンテンツサーバ 20 b は、秘密鍵 x A を設定し（ステップ S 211）、一方で、端末 30 c は、秘密鍵 x B を設定する（ステップ S 212）。

コンテンツサーバ 20 b 及び端末 30 c は、共に管理センタから、楕円曲線 E : $y = x^3 + a x + b$ と元 G とを取得する（ステップ S 213 及びステップ S 214）。

コンテンツサーバ 20 b は、公開鍵 $Y A = x A * G$ を算出する（ステップ S 215）。コンテンツサーバ 20 b は、算出した公開鍵 Y A を分割して、図 20 (a)

に示す様に、IPヘッダのTTLを「1」に設定した公開鍵パケットを生成する（ステップS217）。コンテンツサーバ20bは、生成した公開鍵パケットを順次端末30cへ送信し、端末30cは、公開鍵パケットを受信する（ステップS219）。

5 端末30cは、公開鍵 $YB = xB * G$ を算出する（ステップS216）。端末30cは、算出した公開鍵 YB を分割して、図20（b）に示す様に、IPヘッダのTTLを「1」に設定した公開鍵パケットを生成する（ステップS218）。端末30cは、生成した公開鍵パケットを順次コンテンツサーバ20bへ送信し、コンテンツサーバ20bは、公開鍵パケットを受信する（ステップS220）。

10 コンテンツサーバ20bは、受信した公開鍵パケットに含まれるTTLを確認し（ステップS221）、確かにTTLが「1」である場合（ステップS223でYES）、ステップS211で設定した秘密鍵 xA と、受信した公開鍵 YB とから、共有鍵 $xA * YB$ を算出する（ステップS225）。TTLが「1」でない場合（ステップS223でNO）、コンテンツサーバ20bは処理を終了する。

15 端末30cは、ステップS219で受信した公開鍵パケットに含まれるTTLを確認し（ステップS222）、確かにTTLが「1」である場合（ステップS224でYES）、ステップS212で設定した秘密鍵 xB と、受信した公開鍵 YA とから、共有鍵 $xB * YA$ を算出する（ステップS226）。TTLが「1」でない場合（ステップS224でNO）、端末30cは処理を終了する。

20 このとき、コンテンツサーバ20bが算出する共有鍵は、 $xA * YB = (xA \times xB) * G$ と変形できる。

一方、端末30cが算出する共有鍵は、

$$\begin{aligned} xB * YA &= (xB \times xA) * G \\ &= (xA \times xB) * G \text{と変形できる。} \end{aligned}$$

25 従って、コンテンツサーバ20bと端末30cとで算出された共有鍵は同一のものであることがわかる。

コンテンツサーバ20bの共有鍵生成部108b、及び、端末30cの共有鍵生成部208cは、それぞれ、算出した共有鍵を内部に格納する。続いて、コンテンツサーバ20bは、図21のステップS203の処理を続け、端末30cはステップS204の処理を続ける。

なお、ステップS203のコンテンツ送信処理は、コンテンツ配信システム1におけるコンテンツ送信処理の動作（図9（a））と同一であるため、説明を省略する。同様に、ステップS204のコンテンツ受信処理は、コンテンツ配信システム1におけるコンテンツ受信処理の動作（図9（b））と同一であるため、説明を省略する。

＜まとめ＞

以上まとめると、上記第1の実施の形態において、コンテンツサーバ20は、端末とのデータ通信における隔たりの量を示す通信距離として、端末から受信するパケットに設定されたTTLを用いて、前記端末がAD内の端末であるか、又は、AD外の端末であるか判定する。

コンテンツ配信システム1において、各端末は、TTLが「1」であるコンテンツサーバ検索パケットをマルチキャスト送信する。コンテンツサーバ検索パケットは、各端末が接続されているルータを越えて他のサブネットワークへ送信されない。そのため、コンテンツサーバ20は、自身と同じルータ下に接続されている端末30から送信されたコンテンツサーバ検索パケットのみを受信する。

コンテンツサーバ20は、コンテンツサーバ検索パケットを受信すると、TTLが「1」である確認パケットを返送する。確認パケットは、コンテンツサーバ20が接続されているルータを越えて他のサブネットワークへ送信されない。そのため、端末40及び端末50が、不正に確認パケットを受信することは出来ず、確かに同じルータ下に接続されている端末30のみが確認パケットを受信することができる。

また、コンテンツサーバ20と端末30とは、DFビットを「有効」に設定し、且つ、MTUに等しいデータサイズにパディング処理を施したパケットを送受信することで伝送経路上の他の端末、特に不正な端末によりIPパケットに不必要な情報が付加されて、不正な端末へパケットが転送されるのを抑止する。

また、端末30は、パケットのIPペイロードに自身が接続されているルータのMACアドレスを包含して送信することにより、コンテンツサーバ20は、端末30が確かに自身と同じルータに接続されていることを確認することができる。

上記第1変形例において、コンテンツサーバ20aと端末30とは、複数個の中継機器を介して接続されている。端末30は、コンテンツサーバ20aから応答が

あるまで、TTLを最小値の「1」から1ずつ増加させたTTL検索パケットをマルチキャスト送信する。端末30は、TTLを「n」に設定したTTL検索パケットをマルチキャスト送信した後、コンテンツサーバ20から確認パケットを受信した場合、コンテンツサーバ20aと通信を行うために必要な最小のTTLは「n」であると判断する。以後、端末30とコンテンツサーバ20aとは、TTLを「n」に設定したパケットを送受信することにより、鍵共有処理及びコンテンツ送受信処理を行う。

上記第2変形例において、コンテンツ配信システム1bは、コンテンツサーバ20b及び端末30cが、共に互いのIPアドレスを既知である場合に、コンテンツ配信システム1で行うコンテンツサーバ検索処理を省略し、更に、鍵共有処理で送受信する公開鍵パケットのTTLを「1」に設定することで、公開鍵を交換しながらAD判定処理を行うことだ可能なシステムである。

なお、上記第2変形例において、公開鍵パケットに設定されるTTLは必ずしも「1」である必要はない。例えば、コンテンツサーバ20bと端末30cとの間で任意の「n」をTTLに設定し、双方が受信したパケットのTTLが「n」以下であることを確認することによりAD判定を行ってもよい。

また、図22のステップS222及びステップS224の処理は、必ずしも必要ではない。コンテンツサーバ20bのみが、受信したパケットのTTLが「1」であることを確認する構成であってもよい。

更に、第2変形例において、コンテンツサーバ20bのAD判定部106bは、内部にCRLを格納しており、端末30cから受信する公開鍵パケットに含まれる端末30cの機器IDを読み、読み出した機器IDが、CRLに含まれるか否か判定してもよい。上記判定により端末30cの機器IDが、CRLに含まれる場合には、コンテンツサーバ20bは、公開鍵パケットの送信処理を抑制するように構成されてもよい。

《第2の実施の形態》

本発明に係る第2の実施の形態として、コンテンツ配信システム2について、図面を参照して説明する。コンテンツ配信システム2は、コンテンツ配信システム1と同様に、端末から送信されるパケットに含まれるTTLを用いて、前記端末がA

D内の端末であるか否かを判定する。コンテンツ配信システム1は、AD内の端末であると判定された端末とサーバとが鍵を共有する構成を有していたが、コンテンツ配信システム2は、AD内の端末であると判定された端末を、サーバがグループに登録する構成を有する。

- 5 なお、コンテンツ配信システム2において、各機器は通信プロトコルとしてIPv4を使用して通信を行うものとする。

＜構成＞

- 10 図23は、コンテンツ配信システム2の構成を示す図である。コンテンツ配信システム2は、ルータ10、ルータ11、ルータ12、コンテンツサーバ20a、端末30、端末40及び端末50から構成される。ルータ10、ルータ11、ルータ12、端末30、端末40及び端末50は、コンテンツ配信システム1（図1）と同一の構成及び機能を有するためコンテンツ配信システム1と同一の符号を付して説明を省略する。ここでは、コンテンツ配信システム1と異なる機能を有するコンテンツサーバ20aについて説明する。

- 15 図24は、コンテンツサーバ20aの構成を示すブロック図である。同図に示す様に、コンテンツサーバ20aは、通信部101、暗号処理部102、機器ID管理部103、中継機器固有情報取得部104、最大伝送量探査部105、AD判定部106、確認情報生成部107、グループ管理部108a及びコンテンツ格納部109から構成される。なお、図24において、コンテンツサーバ20（図2）と同一の機能を有する構成要素には、同一の符号を付し、説明を省略する。
- 20

- グループ管理部108aは、AD判定部106によりAD内の端末であると判定された端末、即ち、グループ内端末の情報を管理する。より具体的には、グループ管理部108aは、AD判定部106から指示を受け、コンテンツ要求IDを生成する。グループ管理部108aは、生成したコンテンツ要求IDを、グループ内端末に送信する。また、グループ管理部108aは、生成した前記コンテンツ要求IDと前記グループ内端末の機器IDとを対応付けて、図25に示すグループテーブル350に登録する。
- 25

 図25に示したグループテーブル350は、AD判定部106によりAD内の端末であると判定された全ての端末について、機器IDとコンテンツ要求IDとが対

応付けられて構成されており、例えば、機器ID「ID_E」に対応付けられているコンテンツ要求IDは、「CID_0001」である。同様に、機器ID「ID_F」に対応付けられているコンテンツ要求IDは、「CID_0002」である。

5 また、グループ管理部108aは、端末から、当該端末の機器IDと当該端末が有するコンテンツ要求IDとを含むコンテンツ送信要求を受け付けると、前記機器IDと前記コンテンツ要求IDとがグループテーブル350に登録されているか否か判断する。

10 グループ管理部108aは、前記機器IDと前記コンテンツ要求IDとがグループテーブル350に登録されていると判断すると、コンテンツ格納部109からコンテンツを読み出し、読み出したコンテンツを通信部101を介して端末へ送信する。

<動作>

15 図26(a)及び図26(b)に示すフローチャートを用いて、コンテンツ配信システム2の動作について説明する。なお、図26(a)及び図26(b)のフローチャートは、コンテンツサーバ20a及び端末30の動作のみを記載しているが、端末40及び端末50は、端末30と同様に動作するため、ここでは、コンテンツサーバ20a及び端末30の動作のみを記載している。

 図26(a)は、コンテンツ配信システム2におけるグループ登録処理の動作を示すフローチャートである。

20 先ず、端末30で要求が発生すると(ステップS131)、コンテンツサーバ20aと端末30との間でAD判定処理を行う(ステップS132)。なお、ステップS132の詳細は、図6及び図7に示した動作と同一であるので説明は省略する。

25 続いて、コンテンツサーバ20aは、コンテンツ要求IDを生成し(ステップS133)、生成したコンテンツ要求IDを端末30へ送信し、端末30は、コンテンツ要求IDを受信する(ステップS134)。

 コンテンツサーバ20aのグループ管理部108aは、ステップS133で生成したコンテンツ要求IDと、端末30の機器IDとを対応付けてグループテーブル350に登録する(ステップS135)。端末30は、ステップS134で受信したコンテンツ要求IDを、機器ID管理部203に格納する(ステップS136)。

図26(b)は、コンテンツ配信システム2における、コンテンツ要求処理の動作を示すフローチャートである。

5 5 3は、端末30で要求が発生すると(ステップS141)、機器ID管理部203は、内部に格納している機器IDとコンテンツ要求IDとを読み出し(ステップS142)、通信部201を介して読み出した機器IDとコンテンツ要求IDとをコンテンツサーバ20aへ送信する(ステップS143)。コンテンツサーバ20aの通信部101は、端末30から送信された機器IDとコンテンツ要求IDとを受信する(ステップS143)。

10 コンテンツサーバ20aのグループ管理部108aは、内部に格納しているグループテーブル350を読み出し(ステップS144)、ステップS143にて端末30から受信した機器IDとコンテンツ要求IDとが、グループテーブル350に登録されているか否か判断する。

15 機器IDとコンテンツ要求IDとがグループテーブル350に登録済みである場合(ステップS145でYES)、グループ管理部108aは、コンテンツ格納部109からコンテンツを読み出す(ステップS146)。グループ管理部108aは、読み出したコンテンツを通信部101を介して端末30へ送信し、端末30は、コンテンツを受信する(ステップS147)。端末30は、受信したコンテンツを再生するか、又は、記憶部209へ格納する(ステップS148)。

20 機器IDとコンテンツ要求IDとが登録済みでない場合(ステップS145でNO)、コンテンツサーバ20aは処理を終了する。

<まとめ>

25 第2の実施の形態をまとめると、通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する取得手段と、取得した前記通信距離が、所定値以下であるか否か判定する判定手段と、前記判定の結果が肯定的である場合に、前記他の通信装置をグループに登録する登録手段とを備えることを特徴とする通信装置である。

前記通信手段は、前記他の通信装置とデータの通信を行い、前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数を示す前記通信距離を取得することを特徴とする。

前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数として、前記データが経由したルータの数を示す前記通信距離を取得することを特徴とする。

5 前記通信手段は、ルータを一つ経由する毎に1ずつ値が減少する性質を有するTT Lを含むパケットの形式で、前記データの通信を行い、前記取得手段は、前記通信手段が受信するパケットに含まれる前記TT Lを用いて、前記データが経由したルータの数を示す前記通信距離を取得することを特徴とする。

10 前記通信手段は、前記他の通信装置から、当該他の通信装置が接続されている第1のルータを一意に識別する第1識別情報を含む前記パケットを受信し、前記通信装置は、更に、当該通信装置が接続されている第2のルータを一意に識別する第2識別情報を取得するルータ情報取得手段と、前記第1識別情報と前記第2識別情報が一致するか否か判断する判断手段と、前記判断手段による判断の結果が否定的である場合に、前記通信手段による前記コンテンツの送受信を抑制する抑制手段とを備えることを特徴とする。

15 前記通信手段が送受信する各パケットは、当該通信手段が接続されているネットワークの最大伝送量 (Maximum Transmission Unit) に等しいデータサイズであり、且つ、分割して送受信することが禁止されていることを特徴とする。

20 前記通信手段は、前記他の通信装置から、送信時に所定TT Lが設定されて送信されたパケットを受信し、前記取得手段は、前記通信手段が受信した前記パケットからTT Lを読み、読み出したTT Lと前記所定TT Lとの差分である前記通信距離を取得することを特徴とする。

前記通信手段は、前記他の通信装置から、送信時に前記所定TT Lとして「1」が設定されて送信された前記パケットを受信することを特徴とする。

25 前記通信機器は、前記登録手段によりグループに登録された他の通信機器に対してコンテンツを送信するコンテンツ送信手段を備えることを特徴とする。

また、第2の実施の形態は、第1の通信機器と、1以上の中継機器を介して接続された第2の通信機器とから構成されるグループ登録システムであって、前記第1の通信機器から登録要求を受け付けると、前記第2の通信機器とのデータ通信における隔たりの量を示す通信距離を取得する取得手段と、取得した前記通信距離が、

所定値以下であるか否か判定する判定手段と、前記判定の結果が肯定的である場合に、前記第２の通信機器をグループに登録する登録手段を備え、前記第２の通信機器は、前記第１の通信機器に対して登録要求を送信することを特徴とする。

《その他の変形例》

- 5 なお、本発明を上記第１の実施の形態、その変形例及び第２の実施の形態に基づき説明してきたが、本発明がこれらの実施形態に限定されないのは勿論であり、以下の様な場合も本発明に含まれる。

10 （１）上記実施の形態では、コンテンツサーバは、前記端末から受信するパケットに含まれるＴＴＬを用いて、ＡＤ内の端末であるか、又は、ＡＤ外の端末であるか判定しているが、コンテンツサーバにおけるＡＤ判定方法は、これに限定されない。例えば、コンテンツサーバは、コンテンツサーバと端末との長さを測定し、測定した長さに基づきＡＤ判定してもよい。また、コンテンツサーバは、コンテンツサーバと端末との間の通信に要する時間を測定し、測定した時間に基づきＡＤ判定してもよい。なお、これらの測定方法については限定されない。

15 （２）上記実施の形態において、コンテンツ配信システムに含まれる各機器は、ＩＰｖ４のプロトコルで通信を行う構成を有しているが、本発明において、通信プロトコルはＩＰｖ４に限定されないのは勿論である。例えば、ＩＰｖ６のプロトコルで通信を行う構成も本発明に含まれる。この場合、ＩＰｖ４のＴＴＬフィールドに替えて、ＩＰｖ６のＨｏｐ Ｌｉｍｉｔフィールドを利用してＡＤ判定を行ってもよい。

20 （３）上記第１の実施の形態では、各機器は、ＴＴＬが「１」であるパケットを送受信する構成を有しているが、本発明において、ＴＴＬフィールドに設定するＴＴＬは「１」に限定されないのは勿論である。

25 第１の実施の形態においては、例えば、コンテンツサーバと端末との間で所定のＴＴＬ値（ここでは１０とする）をＴＴＬフィールドに設定するように予め決めておく。端末は、ＴＴＬを「１０」に設定したコンテンツサーバ検索パケットをマルチキャスト送信する。コンテンツサーバは、コンテンツサーバ検索パケットを受信すると、ＴＴＬフィールドに含まれるＴＴＬが所定値「１０」からの増減が無いか、を確認しＴＴＬが「１０」である場合に、当該端末と鍵共有処理を行うように構成

してもよい。

(4) 上記実施の形態において、端末30はルータ11に直接接続される構成を有しているが、本発明はこの構成に限定されず、例えば、端末30とルータ11とがスイッチやハブなどを介して接続される構成も本発明に含まれる。

5 (5) 上記実施の形態では、IPパケットの送信時と受信時とにおける、TTLの減少量が「0」の場合をAD内と判定しているが、例えばIPパケットの送信時と受信時とにおけるTTLの減少量が「所定値以下」の場合をAD内と判定することでADを任意に広げることが可能である。例えば、TTLの減少量が「2」である端末までAD内端末であるとしてもできる。

10 (6) 上記第1の実施の形態及びその変形例において、コンテンツサーバから暗号化コンテンツを受信した端末は、前記暗号化コンテンツを復号した後、記憶部に格納する構成を有しているが、端末は、復号したコンテンツを再生する構成も本発明に含まれる。

15 (7) 上記実施の形態において、IPパケットのIPペイロードを暗号化したり復号したりするときに暗号処理部で用いる暗号鍵は、グローバルシークレットな値としているが、必ずしもこれに限定されず、例えば事前にゼロ知識証明を利用したチャレンジ-レスポンス型のハンドシェイクを行い、セッション鍵を共有する方法であってもよい。

20 (8) 上記実施の形態において、各機器は、MTUに等しいデータサイズのパケットを送受信する構成を有しているが、各機器は、必ずしもMTUに等しいデータサイズのパケットを送受信する必要は無く、データサイズがMTUと異なるパケットを送受信する構成も本発明に含まれる。

25 (9) 上記実施の形態において、各機器は、DFビットを「有効」に設定したパケットを送受信する構成を有しているが、各機器は、必ずしもDFビットを「有効」に設定したパケットを送受信する必要は無く、DFビットが「無効」の場合であっても本発明に含まれる。

(10) 上記実施の形態において、各機器は、自身が接続されている中継機器を識別する中継機器固有情報を取得し、取得した中継機器固有情報を含むパケットを送信する構成を有しているが、各機器は、必ずしも中継機器固有情報を含んだパケ

ットを送信する必要は無い。各機器は、中継機器固有情報を含まないパケットを送受信する構成も本発明に含まれる。

5 (11) 上記の実施の形態では、端末の機器IDをグループテーブルに登録する構成を有しているが、本発明は、これに限定されず、例えば、端末に装着して用いるメモリカードなどの記録媒体のIDをグループテーブルに登録するような場合も含まれる。

(12) また、本発明は、コアCPUとDSPとにより構成されるシステムLSIであってもよい。前記システムLSIが、DPSプログラムであるコンテンツ配信プログラムを実行する構成も本発明に含まれる。

10 (13) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、
15 CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気
20 通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

25 また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(14) 上記実施の形態及び上記変形例をそれぞれ組み合わせる構成も本発明に

含まれる。

産業上の利用の可能性

- 5 上記において説明したコンテンツ配信システムは、映画、音楽などのデジタル化された著作物を、放送やネットワークなどを介して流通させる産業において、家庭内においては自由にコンテンツを利用し、家庭外にはコンテンツの流出を防ぐ仕組みとして利用できる。

請 求 の 範 囲

1. 通信装置であって、以下を含む：

・取得手段、

5 当該通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定手段、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信手段、

10 前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの送信又は受信を行う。

2. 前記通信手段は、前記コンテンツの送信又は受信に先立ち、前記他の通信装置とデータの通信を行い、

15 前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数を示す前記通信距離を取得する

ことを特徴とする請求の範囲 1 に記載の通信装置。

20 3. 前記取得手段は、前記他の通信装置から送信されたデータを当該通信装置が受信するまでの間に、前記データが経由した中継機器の数として、前記データが経由したルータの数を示す前記通信距離を取得する

ことを特徴とする請求の範囲 2 に記載の通信装置。

25 4. 前記通信手段は、ルータを一つ経由する毎に 1 ずつ値が減少する性質を有する TTL (Time To Live) を含むパケットの形式で、前記データの通信を行い、

前記取得手段は、前記通信手段が受信するパケットに含まれる前記 TTL を用いて、前記データが経由したルータの数を示す前記通信距離を取得する

ことを特徴とする請求の範囲 3 に記載の通信装置。

5. 請求の範囲 4 に記載の通信装置は、更に、以下を備える：

- ・ 鍵共有手段、

前記他の通信装置と鍵情報を共有する。

5 6. 請求の範囲 5 に記載の通信装置は、更に、以下を備え：

- ・ 暗号処理手段、

前記鍵共有手段により前記他の通信装置と共有した前記鍵情報を用いて、前記コンテンツの暗号化処理及び暗号化された前記コンテンツの復号処理を行う；

前記通信手段は、前記他の通信装置との間で、前記暗号処理手段により暗号化された前記コンテンツの送信又は受信を行う。

10

7. 請求の範囲 6 に記載の通信装置であって、

前記通信手段は、前記他の通信装置から、当該他の通信装置が接続されている第 1 のルータを一意に識別する第 1 識別情報を含む前記パケットを受信し、

15 当該通信装置は、更に、以下を含む：

- ・ ルータ情報取得手段、

当該通信装置が接続されている第 2 のルータを一意に識別する第 2 識別情報を取得する；

- ・ 判断手段、

20 前記第 1 識別情報と前記第 2 識別情報とが一致するか否か判断する；

- ・ 抑制手段、

前記判断手段による判断の結果が否定的である場合に、前記通信手段による前記コンテンツの送受信を抑制する。

25 8. 前記通信手段が送受信する各パケットは、当該通信手段が接続されているネットワークの最大伝送量 (Maximum Transmission Unit) に等しいデータサイズであり、且つ、分割して送受信することが禁止されている

ことを特徴とする請求項 7 に記載の通信装置。

9. 前記通信手段は、前記他の通信装置から、送信時に所定TTLが設定されて送信されたパケットを受信し、

前記取得手段は、前記通信手段が受信した前記パケットからTTLを読み、読み出したTTLと前記所定TTLとの差分である前記通信距離を取得する

5 ことを特徴とする請求の範囲8に記載の通信装置。

10. 前記通信手段は、前記他の通信装置から、送信時に前記所定TTLとして「1」が設定されて送信された前記パケットを受信する

ことを特徴とする請求の範囲9に記載の通信装置。

10

11. 前記通信手段は、一部又は全部が暗号化されたパケットを送信又は受信し、
前記暗号処理部は、前記通信手段が受信した前記パケットを復号して前記取得手段へ出力し、又は、前記通信手段により送信されるパケットを暗号化して前記通信手段へ出力する

15 ことを特徴とする請求の範囲10に記載の通信装置。

12. 前記取得手段は、当該通信装置と前記他の通信装置との間の長さを示す前記通信距離を取得する

ことを特徴とする請求の範囲1に記載の通信装置。

20

13. 前記取得手段は、当該通信装置と前記他の通信装置との間のデータ通信に要する時間を示す前記通信距離を取得する

ことを特徴とする請求の範囲1に記載の通信装置。

25 14. 送信装置から受信装置へ、コンテンツを送信するコンテンツ配信システムであって、

前記送信装置は、以下を含み：

・取得手段、

前記受信装置とのデータ通信における隔たりの量を示す通信距離を取得する；

・判定手段、

取得した前記通信距離が、所定値以下であるか否か判定する；

・送信手段、

前記判定の結果が肯定的である場合に、前記受信手段にコンテンツを送信する；

5 前記受信装置は、前記送信装置から送信される前記コンテンツを受信する。

1 5. 通信装置で用いられるコンテンツ配信方法であって、以下を含む：

・取得ステップ、

前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離

10 を取得する；

・判定ステップ、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信ステップ、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの

15 送信又は受信を行う。

1 6. 通信装置で用いられるコンテンツ配信プログラムであって、以下を含む：

・取得ステップ、

前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離

20 を取得する；

・判定ステップ、

取得した前記通信距離が、所定値以下であるか否か判定する；

・通信ステップ、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの

25 送信又は受信を行う。

1 7. 通信装置で用いられるコンテンツ配信プログラムを実行するLSIであって、

前記コンテンツ配信プログラムは、以下を含む：

・取得ステップ、

前記通信装置と他の通信装置とのデータ通信における隔たりの量を示す通信距離
を取得する；

- ・判定ステップ、

取得した前記通信距離が、所定値以下であるか否か判定する；

5

- ・通信ステップ、

前記判定の結果が肯定的である場合に、前記他の通信装置との間でコンテンツの
送信又は受信を行う。

10

要 約 書

通信途中でコンテンツを盗まれる危険度が高い状況ではコンテンツの送信を抑制するコンテンツ配信システムを提供することを目的とする。

- 5 コンテンツサーバは、端末とのデータ通信における隔たりの量を示す通信距離を取得し、前記通信距離が所定値以下である場合に、コンテンツを送受信し前記通信距離が所定値より大きい場合に、コンテンツの送受信を抑制する。